REMARKS

This application has been carefully considered in connection with the Examiner's Office Action dated September 27, 2007. Reconsideration and allowance are respectfully requested in view of the following.

Summary of Rejections

Claims 1-33 were pending at the time of the Office Action.

Claims 1-3, 4-7, 8, 9-12, 13-14, 15, 16-19, 20, 21-23, 24, 25, 26-27, 28, 29, 30-33 were rejected under 35 USC §103.

Summary of Response

Claims 1, 3, 9, 10-11, and 28 are currently amended herein.

Claims 2, 4-8, 12-27, 29-33 remain as originally submitted.

Remarks and Arguments are provided below.

Summary of Claims Pending

Claims 1-33 are currently pending following this response.

Response to Rejections

The pending application relates to systems and methods for providing application-to-application enterprise security. The system includes a security application program interface, an authentication authority, a store maintaining data, an application program interface, and a server application. The security application program interface is coupled

to a client application to provide a security credential. The authentication authority receives the security credential from the security application program interface and, if the security credential is valid, it generates a token and communicates the token to the security application program interface. The store maintaining the data, which is in communication with the authentication authority, validates the security credential. The application program interface is coupled to the client application and can communicate regarding the token. The server application receives the token from the application program interface and communicates with the authentication authority to validate the token to enable the client application to use services of the server application. This approach to providing application-to-application enterprise security permits the communication of security information in a heterogeneous computing environment using a token encoded as a primitive data type.

With regard to the art rejections, the Office Action has rejected the pending claims citing Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck"). Upton relates to systems and methods for integration adapter security. Beck relates to methods and apparatus for providing anonymity to end users in web transactions. Neither Upton nor Beck disclose using a token which is generated to provide authentication information. In addition, the computing environments in Upton require a homogeneous computing environment, whereas the tokens found in the present disclosure permit the authentication of users in a heterogeneous computing environment.

This distinction, as well as others, will be discussed in greater detail in the analysis of the present claims that follows.

Response to Rejections under Section 103

In the Office Action dated September 27, 2007, Claims 1-3, 9-12, 24, 28 and 29 were rejected under 35 USC § 103(a) as being unpatentable over Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck").

Claim 1, 9, 28:

I. THE "TOKEN" DISCLOSED BY BECK CANNOT BE USED TO PROVIDE USER CREDENTIALS.

Amended Claims 1, 9, and 28 each contain the limitation of "wherein the token contains user credentials encoded as a platform and application independent primitive data type." This amendment is supported by the original specification, as discussed in paragraphs [0028], [0031], and [0032]. Paragraph [0028] discloses the use of a primitive data type that is both platform and application independent.

> [0028] Rather than security information being converted from the format of one platform to the format of another, security information is passed between applications *in the form of a token with a string data type. Since a string is a primitive data type*, it can be recognized by a large number of applications and interfaces, meaning it can be sent over multiple services such as J2EE, CORBA, and IBM's MQSeries. *Making the token a string makes it platform and technology independent because the token has no header and therefore no application-specific header configuration.* [Emphasis Added]

Paragraph [0031] discloses the use of a user credentials with a token.

> [0031] The central authentication and validation authority authenticates the client by verifying the security credentials. In the case of an ID and password, the verification can consist of confirming that the password is valid for the ID. For an X.509 certificate, verification might include determining whether the certificate is trusted, ensuring that the certificate has not expired or been revoked, and determining whether the digital signature within the certificate is valid. *If the security credentials indicate that the application is authentic, the central authentication and validation authority creates a token containing a stringified version of the credentials and returns the token to the client.* [Emphasis Added]

One of the innovative features of this security token is the ability to use a primitive data type to identify a particular user thereby creating a platform and application independent security procedure. In large heterogeneous computing environments, this approach removes the need to have security interpreters, decoders, and converters that are application and platform specific greatly increasing the interoperability of computing networks.

The Office Action notes that Upton does not teach using a token as security credentials, and attempts to use Beck to cure this deficiency. However, the token disclosed by Beck is not the same as the claimed token. The token disclosed by Beck is intended to remove identifying features and create anonymity in internet transactions, whereas the claimed token is used to securely identity users. The title of the Beck application is "Method and apparatus for providing anonymity to end-users in web transactions" and the lack of user identifying information is disclosed in paragraph [0015] of Beck.

> [0015] If rule engine 201 determines from its destination URL that the end-user-originated request requires the inclusion of an HTTP header containing a temporary user ID token before being forwarded to its destination, then a specific service module 206 is invoked that can generate that token and insert an HTTP header containing that token and other information into the request. **That service module 206 thus generates a random or pseudo-random token that is meaningless on its own**, but indicates to the ISP the identity of the particular end-user who originated the request." [Emphasis Added]

The token used by Beck does not contain "user credentials encoded as a platform and application independent primitive data type" as disclosed by independent Claims 1, 9, and 28. Therefore, the token disclosed in Beck cannot be used to authenticate users based upon user credentials, because the token of Beck contains only "meaningless" information. Therefore, the token of Beck does not teach or suggest a token containing user credentials encoded as a platform and application independent primitive data type.

II. THE COMBINATION OF UPTON AND BECK WOULD CREATE AN INSECURE COMPUTING PLATFORM AND NOT AN APPLICATION-TO-APPLICATION SECURE ENVIRONMENT.

The present disclosure provides application-to-application enterprise security that permits the communication of security information in a heterogeneous computing environment using a token encoded as a primitive data type. This feature allows for disparate computers, platforms, and networks to securely exchange information without the need for individual encoding, decoding, and converting modules. This also ensures

that resources are secured properly and that only users that have access permissions to resources can access those resources.

A combination of Upton and Beck would not form the presently claimed invention in Claims 1, 9, and 28. Instead, a combination of Upton and Beck would result in a system that was unable to authenticate any user. Upton has the specific requirement, as explained in paragraph [0073], that users must be authenticated by the server to which they are being connected. For the purpose of clarity, paragraph [0073] of Upton recites:

> [0073] Application/integration server users typically must be authenticated whenever they request access to a protected server resource. For this reason, each user can be required to provide a credential, such as a username/password pair or a digital certificate.

In contrast, Beck strips the user identifying information from transactions replacing user identifying information with pseudo random tokens. Beck is directed towards anonymity in web transactions (as previously discussed) that removes the username/password of a particular user. Therefore, a combination of Upton, which requires user authentication, and Beck, which removes user information, creates a system that could not authenticate any user. It is therefore respectfully submitted that a combination of Upton and Beck would create a system that does not teach or suggest the claimed systems and methods for providing application-to-application enterprise security.

III. Neither Beck Nor Upton Contemplate Using a Primitive Data Type to Exchange Security Information Among Heterogeneous Applications and Platforms.

Amended Claims 1, 9, and 28 each contain the limitation of "wherein the token contains user credentials encoded as a platform and application independent primitive data type." This primitive data type is important because it permits the exchange of user information without the need for conversion throughout disparate systems and platforms. Both Upton and Beck only contemplate homogenous network environments, whereas the pending application contemplates heterogeneous computing environments. This is discussed throughout the pending application, including paragraphs [0025] and [0027] of the pending application.

> [0025] ...In a heterogeneous environment of disparate applications, however, one application typically cannot recognize the format of the messages from another application. Thus, in order for security information to be passed from one application to another, the header would have to be converted from the format of one application to the format of the other application. If multiple disparate applications were present, a converter would be needed between every possible combination of different applications. The labor and expense needed to create and implement a large number of converters could be significant.
> [0027] The present system allows tokens to be passed among disparate applications so that security information can automatically be included with each call from one application to another. This eliminates the need for conversion of security information in message headers between the data formats of the applications. It also eliminates the need for an application to be authenticated and authorized every time it sends a message to another application. In contrast with services where a security context remains present on a server, in embodiments of the invention there is no permanent context or session. Instead, a context is created with every invocation from one application to another.

Since nether Upton nor Beck contemplate the use of a primitive data type which removes the need for conversion of security information in a heterogeneous computing environment, it is respectfully submitted that Upton and Beck do not teach or suggest the limitation of "the token contains user credentials encoded as a platform and application independent primitive data type" found in Independent Claims 1, 9, and 28.

For at least the reasons established above in sections I-III, Applicants respectfully submit that independent Claim 1 is not taught or suggested by Upton or Beck and respectfully request allowance of this Claim.

Dependent Claims 2-3 depend directly or indirectly from independent Claim 1 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 2-3 are not taught or suggested by Upton or Beck and respectfully request allowance of these claims.

Claim 9:

Claim 9 includes limitations substantially similar to the limitations discussed in sections I-III above. For at least the reasons established above in sections I-III, Applicants respectfully submit that independent Claim 9 is not taught or suggested by Upton or Beck and respectfully request allowance of this claim.

Dependent Claims 10-12 and 24 depend directly or indirectly from independent Claim 9 and incorporate all of the limitations thereof. Accordingly, for at least the

reasons established in sections I-III above, Applicants respectfully submit that Claims 10-12 and 24 are not taught or suggested by Upton or Beck and respectfully request allowance of these claims.

Claim 28:

Claim 28 includes limitations substantially similar to the limitations discussed in sections I-III above. For at least the reasons established above in sections I-III, Applicants respectfully submit that independent Claim 28 is not taught or suggested by Upton or Beck and respectfully request allowance of this claim.

Dependent Claim 29 depends directly or indirectly from independent Claim 28 and incorporates all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claim 29 is not taught or suggested by Upton or Beck and respectfully request allowance of this claim.

Claims Depending from Independent Claims 1, 9, and 28:

In the Office Action dated September 27, 2007, Claims 4-7, 13-14, 16-19, 21-23 and 30-33 were rejected under 35 USC § 103(a) as being unpatentable over Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck") further in view of Gurevich et al., U.S. Publication No. 2002/0178370 (hereinafter "Gurevich").

Dependent Claims 4-7, depend directly or indirectly from independent Claim 1 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 4-7, 13-14

and 16-19 are not taught or suggested by Upton, Beck and Gurevich and respectfully request allowance of these claims.

Dependent Claims 13-14, 16-19 and 21-23 depend directly or indirectly from independent Claim 9 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 13-14, 16-19 and 21-23 are not taught or suggested by Upton, Beck and Gurevich and respectfully request allowance of these claims.

Dependent Claims 30-33 depend directly or indirectly from independent Claim 28 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 30-33 are not taught or suggested by Upton, Beck and Gurevich and respectfully request allowance of these claims.

Claims Depending from Independent Claims 1 and 9:

In the Office Action dated September 27, 2007, Claims 8 and 15 were rejected under 35 USC § 103(a) as being unpatentable over Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck") further in view of Laferriere et al., U.S. Publication No. 2005/0188212 (hereinafter "Laferriere").

Dependent Claims 8 and 15 depend directly or indirectly from independent Claims 1 and 9, respectively and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully

submit that Claims 8 and 15 are not taught or suggested by Upton, Beck and Laferriere and respectfully request allowance of these claims.

Claims Depending from Independent Claim 9:

In the Office Action dated September 27, 2007, Claims 20 and 25 were rejected under 35 USC § 103(a) as being unpatentable over Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck") further in view of Gurevich, et al., U.S. Publication No. 2002-0178370 (hereinafter "Gurevich") further in view of Favazza, et al., U.S. Publication No. 2004/0139319 (hereinafter "Favazza").

Dependent Claims 20 and 25 depend directly or indirectly from independent Claim 9 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 20 and 25 are not taught or suggested by Upton, Beck, Gurevich and Favazza and respectfully request allowance of these claims.

Claims Depending from Independent Claim 9:

In the Office Action dated September 27, 2007, Claims 26 and 27 were rejected under 35 USC § 103(a) as being unpatentable over Upton, U.S. Publication No. 2003/0097574 (hereinafter "Upton") in view of Beck, et al., U.S. Publication No. 2004/0088349 (hereinafter "Beck") further in view of Favazza, et al., U.S. Publication No. 2004/0139319 (hereinafter "Favazza").

Dependent Claims 26 and 27 depend directly or indirectly from independent Claim 9 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-III above, Applicants respectfully submit that Claims 26 and 27 are not taught or suggested by Upton, Beck and Favazza and respectfully request allowance of these claims.

Conclusion

Applicants respectfully submit that the present application is in condition for allowance for the reasons stated above. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, he is encouraged to telephone the undersigned at (972) 731-2288.

The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 21-0765, Sprint.

Respectfully submitted,

Date: December 26, 2007

/Michael W. Piper/
Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5601 Granite Parkway, Suite 750
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)